A Brinkmanship Game Theory Model for Competitive Wireless Networking Environment

Jahan A. Hassan and Mahbub Hassan
School of Computer Science and Engineering
The University of New South Wales
Sydney, NSW2052, Australia
Email{jahan,mahbub}@cse.unsw.edu.au

Sajal K. Das
Department of Computer Science and Engineering
The University of Texas at Arlington,
Arlington, TX 76019-0015
Email: das@cse.uta.edu

***Abstract*—Mobile handset manufacturers are introducing new features that allow a user to configure the same handset for seamless operation with multiple wireless network providers. As the competitiveness in the wireless network service market intensifies, such products will deliver greater freedom for the mobile users to switch providers dynamically for a better price or quality of experience. For example, when faced with an unexpected wireless link quality problem, the user could choose to physically switch the provider, or she could be more strategic and use her freedom of switching provider as a 'psychological weapon' to force the current provider upgrading the link quality without delay. In this paper, we explore the latter option where users threaten to quit the current provider unless he (the provider) takes immediate actions to improve the link quality. By threatening the provider, the user will have to accept the risk of having to disconnect from the current provider and reconnect to another in the middle of a communication session, should the provider defies the threat. The user therefore will have to carefully assess the merit of issuing such threats. To analyze the dynamics of this scenario, we formulate the problem as a brinkmanship game theory model. As a function of user's and provider's payoff or utility values, we derive conditions under which the user could expect to gain from adopting the brinkmanship strategy. The effect of uncertainties in payoff values are analyzed using Monte Carlo simulation, which confirms that brinkmanship can be an effective strategy under a wide range of scenarios. Since user threats must be credible to the provider for the brinkmanship model to work, we discuss possible avenues in achieving threat credibility in the context of mobile communications.**

I. Introduction

Advancements in handset technology, e.g., dual-sim mobile phones [1], together with the growing competition in the wireless network service market are empowering the next generation mobile users with an unprecedented freedom to switch their network provider anywhere anytime to optimize the cost or quality of the wireless connectivity. For example, if the quality of the wireless connection from the current network provider deteriorates, the user could disconnect from the current provider and reconnect through another, hopefully with a better link quality.

We argue that, to benefit from it, the user does not necessarily have to always exercise her freedom of provider switching. The freedom could perhaps be used more strategically as a 'psychological weapon' to force the current provider rectify the link quality problem in the first place [1]. If successful, she could save herself the inconvenience of physically switching provider in the middle of a communication session and enjoy a quality connectivity at the same time. This strategic use of the freedom of provider switching is the focus of this paper. More specifically, we explore the concept where the user threatens to quit the current provider unless he takes immediate actions to improve the link quality. By threatening the provider, the user will have to accept the risk of physically carrying out the undesired action of physically switching the provider should the provider defies the threat. The user therefore will have to carefully assess the merit of issuing such threats.

We analyze the dynamics of the 'psychological war' between the user and the provider over the quality of the wireless connection using brinkmanship game theory. Brinkmanship is a form of diplomatic maneuver generally used in international politics which seeks advantage by creating the impression that one is willing and able to push a highly dangerous situation to the limit and not tolerate it, using *threat* as a strategic move. As a function of user's and provider's payoff or utility values, we derive conditions under which the user could expect to gain from adopting the brinkmanship strategy. The effect of uncertainties in payoff values are analyzed using Monte Carlo simulation, which confirms that brinkmanship can be an effective strategy under a wide range of scenarios. Since user threats must be credible to the provider for the brinkmanship model to work, we discuss possible avenues in achieving threat credibility in the context of mobile communications.

The rest of the paper is organized as follows. Related work is reviewed in Section II. Section III presents the game theoretic analysis of the threat scenario using specific payoff values. In Section IV, we generalize the brinkmanship model for arbitrary payoff values and derive mathematical equations for the key parameters of the model. Section V presents the Monte Carlo simulation and discusses the distributions of critical variables of the brinkmanship model under uncertain

[1]There exists a host of techniques, including increasing the power level [2] or switching to a more robust forward error correction (FEC) algorithm [3], that a provider could use to fix a wireless channel problem. However, fixing a channel quality problem using such techniques would mean allocation of additional radio resources to a suffering user. Given that radio resource is limited, the provider may not always have the incentive to fix the problem.

payoffs. Section VI discusses possible avenues for achieving threat credibility in the context of mobile communications. We conclude in Section VII and discuss directions for future research.

II. Related Work

Game theory [4] has recently become a tool of choice for solving many problems related to wireless network resource and quality management. For example, a cooperative game theoretic framework has been presented in [5] to address the resource allocation problem in heterogeneous wireless networks by forming coalition among them. The coalition structure based cooperative allocation strategy has been shown to maximize network resources while satisfying user performance requirements. Chatterjee et. al. [6] studied the admission control in CDMA systems by modeling the conflicting interest between the provider and users as non-cooperative games. The work presented in [7] models the dynamics of resource sharing where N users share a wireless LAN access point and dynamically select a bit rate for their voice calls. This game models the interactions among the users, but the provider side is not taken into account. Munasinghe et. al. [8] focused on how to compensate a user during the period of total outage in interworked WLAN-3G networks through a non-cooperative game theory based pricing mechanism.

Brinkmanship game theoretic models (strategic moves) [4] have been used primarily to analyze political moves. One classical example of Brinkmanship games is that of the Cuban Missile Crisis. Brinkmanship model has recently been used by Melese et. al. in deterring terrorism [9]. To the best of our knowledge, Brinkmanship has not been applied in the context of wireless networking. In this paper, we make an initial attempt to explore the applicability of Brinkmanship models in the context of competitive wireless networking environment.

III. Game Theoretic Analysis

The user and the provider have conflicting interests in the following sense. The user wants high quality wireless communication links between her mobile handset and the provider's BS, which may cost the provider dearly, while the provider wants to serve as many users as possible with his limited spectral resource in order to generate more revenue. Game theory is an established branch of science that can analyze such conflicts and hint on possible outcomes when everyone behaves rationally to maximize his or her own payoff. In this section, we analyze the proposed user-threatening-the-provider scenario using game theory.

In game theory, threat is considered as one kind of strategic move [4]. Strategic moves are mechanisms that a player can use to manipulate the rules of a game to produce an outcome that is more favourable to her. There are three types of strategic moves a player can choose from: commitments, promises, and threats. In this paper, we will use threat as a strategic move for the user trying to force the provider to fix the link quality problem in a user-provider game. In explaining the threat mechanism, we adopt the examples and style used in [4] for the analysis of the Cuba Missile Crisis involving the Soviets and the US. We begin with the game where no threats are used.

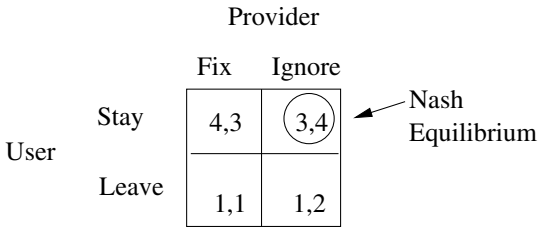


Fig. 1. The Game without Threat: User vs Provider

A. Game with No Threats

There are two players in this game, the user, and the wireless network service provider[2]. When the channel quality degrades, the user can choose from two possible actions, *stay* or *leave*. Similarly, when the channel quality problem is detected, the provider (or the BS) can decide to either *fix* the problem, or *ignore* it. Since wireless resources are limited, we assume that fixing the quality problem with additional resource allocation would have some cost to the provider. We assume that there is some inconvenience for the user to terminate the current session and re-initiate it with another provider. Similarly, the provider is also harmed if the user decides to leave (switch provider). This harm can be explained as a loss of potential further revenue from that user for the current session and the risk of churn.

Figure 1 illustrates the payoff structure for the service quality game between the user and the wireless network service provider. For the user, the best outcome (a payoff of 4) is achieved when the user stays and the link quality is fixed. Similarly, her worst outcome (payoff 1) occurs when she has already decided to leave, irrespective of the decision taken by the provider. As for the provider, the best outcome (payoff 4) is when the user stays and the provider does not fix the link quality. The worst (payoff 1) is when the user leaves despite deciding to fix the line.

It is quite interesting to see that this game has a unique Nash equilibrium at (stay, ignore) with payoff (3,4). In practical terms, it means that for occasional minor wireless link quality problems, the user will tend to stay in the call to avoid the inconvenience of termination and re-initiation of the session, while the provider will ignore such problems. In fact, this outcome probably paints a true picture of the current practice in the so called monopolistic wireless market.

Clearly, in this scenario, the provider has no incentive to try any strategic moves to change the game outcome, because it is already getting the highest possible payoff (of 4). The user, however, can try to gain a 4 instead of 3. This is precisely the motivation for the user to use threats. We will first study a

[2]Although there may be more than one user interacting with the same provider at the same time, we can still use a 2-player game to analyse the impact of using threats.

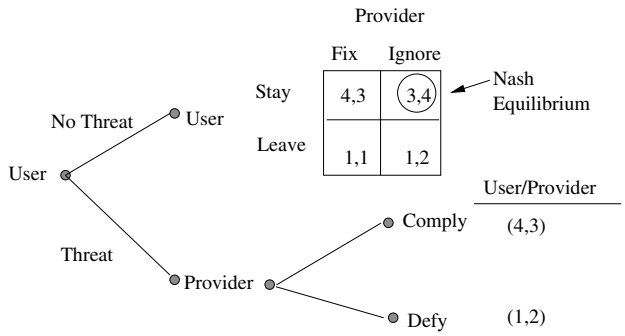


Fig. 2. Game with Pure Threats (Soft Provider)

simple game with *pure* threats, where the threat from the user assumes the rule "fix the link quality immediately, or I will switch to another provider."

B. Game with Pure Threats

The game tree in Figure 2 shows the outcomes when a pure threat is used as a strategic move. The link quality has deteriorated which is simultaneously felt by the user and detected by the provider. As stated earlier, the provider has no incentive to take any action, so it is up to the user to make a strategic move. She can either issue the threat, or do nothing. If the user does not threat, then the original game of the previous section is played and the outcome is the unique Nash equilibrium (3,4). If the user issues the threat, the provider can either comply (fix the quality) or defy (do nothing). If the provider complies, the user stays, which leads to the outcome (4,3). However, if the provider defies the threat, the user hangs up the call, leading to the outcome (1,2).

Given the game tree in Figure 2, we can easily find the subgame-perfect equilibrium. If faced with the user threat, the provider gets 3 from fixing the quality of the wireless connection, but only 2 by defying the threat; so the provider would prefer to comply. Now using the rollback logic, the user works out that she gets 4 by issuing the threat and 3 if she does not. Hence, it is a better strategy for the user to threaten whenever the quality degrades. This way the outcome will be 4 for the user and 3 for the provider, just the opposite of the Nash equilibrium when no threat functions are available in the mobile handset.

One might ask why the providers would comply all the time when they already know that this is a game played by the user to achieve a better outcome at the expense of the provider. Indeed, there is always a risk for the user that a provider may not comply to such threats. When such risks exist, the cost of executing a threat becomes an important consideration for the user. Is there any mechanism for the user to reduce the risk of threats? We answer this question in the following section using the notion of *probabilistic threat* (also known as *brinkmanship*).

C. Game with Probabilistic Threats

Before we introduce the notion of probabilistic threat, let us first analyze some of the limitations of a pure threat. These limitations will serve as a motivation for probabilistic threats.

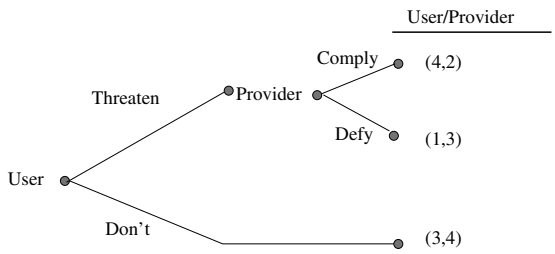


Fig. 3. The Game with hard provider

The conclusion drawn in the previous section about the guaranteed improvement in the user outcome by issuing a threat was based on the assumption that the provider would always comply to such threats because of his payoff structure. Now suppose that the provider's payoffs from compliance and defiance are *opposite* from what they were before, say 2 for complying and 3 for defying. This alternative payoff structure may represent a provider who is experiencing severe shortage of wireless resources. Under such situations, the cost of additional resources needed to address the quality problem outweighs the cost of losing the user hence the reversal of the payoffs. Figure 3 shows the game tree for this case. Now if the user issues a threat, the provider defies it. Therefore, by issuing a threat, the user gets a payoff of only 1, whereas she could get 3 if she did not issue the threat. This analysis shows that, when one cannot be certain about the current resource state of the provider, which dictates the payoff structure of the provider, issuing a pure threat can be too risky.

So far we have found that the user should issue the threat if she knows for sure that the provider has the payoff structure of Figure 1, and similarly, if she knows for sure that the provider has the opposite payoff structure, she must stay away from threatening the provider. In reality, however, the user will not know for sure the current state and payoff structure of the provider. This is where we can use probability to analyse the outcome of the game. Let us say that the provider can be in one of two states, *hard* (severe shortage of resource) and *soft* (resource is limited, but not experiencing severe shortage). Note that, even a soft provider would not automatically fix a quality problem unless threatened because resources are always limited and any additional allocation of resource to an existing user directly increases blocking probability of new users (see the Nash Equilibrium discussed in Section III-A). Let us denote the probability of the provider being hard by p and analyze the consequences as a function of p.

The tree for this more complex game is shown in Figure 4. The game starts with an outside force ('nature') determining the type of the provider the user is dealing with. The upper branch represents the provider being hard and the lower branch the opposite (soft). The user can look ahead and find that, if she issues the threat, she will get a 1 with probability p and a 4 with probability $(1-p)$. The expected payoff from making the threat therefore is $p+4(1-p) = 4-3p$. On the other hand,

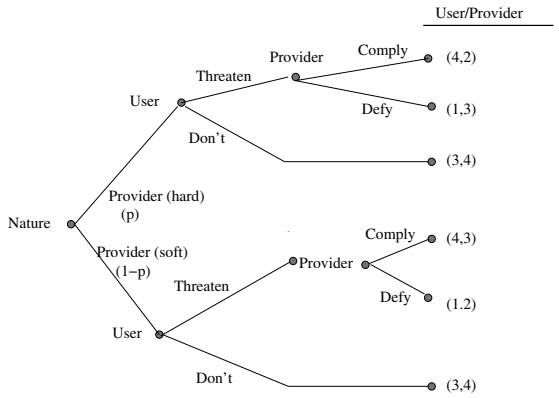


Fig. 4. The Game with Unknown Provider Payoff

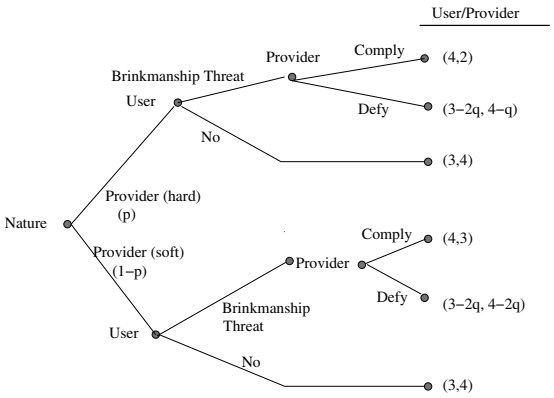


Fig. 5. The Brinkmanship Model of the Game

if the user decides not to push the threat button, her expected payoff is 3 (she gets 3 from either branch). Therefore, for the user, making the threat is useful only if $4-3p>3$, or $p<\frac{1}{3}$.

Under these circumstances, if the user estimates that p is definitely smaller than $1/3$, she should go ahead and push the threat button. However, if she estimated that p could be somewhere say between $1/2$ to $3/4$, the pure threat of "fix the link quality immediately, or I will switch to another provider" is too large, too risky, and too costly for her to make.

Now we are ready to study the notion of a probabilistic threat. The main motivation for probabilistic threat is that it keeps a threat architecture useful even under the circumstances when p is found to be too large for a pure threat to be effective. With a probabilistic threat, the threat signal now reads as "fix the link quality immediately, or I may switch to another provider". Note that the threat has been made probabilistic by replacing "will" with "may". It can be implemented by introducing another probability q as shown in Figure 5. Now, if the provider defies the threat, the user leaves only with probability q and stays with $(1-q)$. Therefore, nobody can be sure about the precise outcome of the game if the provider defies the threat. For the user, the outcome is 1 with probability q and 3 with $(1-q)$, so the expected payoff is $q+3(1-q)=3-2q$.

For the provider, the expected payoff depends on whether he is hard or soft. For hard, he gets 3 if the user executes the threat, which happens with probability q, and a 4 if the user decides not to carry out the threat (stay), which has a probability of $(1-q)$. The expected payoff for hard provider is therefore $3q+4(1-q)=4-q$ if they defy. If the provider were to comply, he would get a 2, which is smaller than $4-q$ irrespective of the value of q in the range 0 to 1. Therefore, the hard provider will defy the threat.

Similarly, it can be shown that the expected payoff for soft provider is $4-2q$ if he defies the threat, and 3 if it complies. In this case, compliance is better if $3>4-2q$, or $q>0.5$. Therefore, the user should execute its threat, i.e., leave current provider, with at least 50% probability, otherwise, it will not be able to deter the providers at all, even the soft types (Note that Figure 4 can be thought of an extreme case of probabilistic threat with $q=1$). This lower bound on q is called the *effectiveness condition* for a probabilistic threat. It is called so, because if q is smaller than this lower bound, both type of providers, soft and hard, will defy the threat making the threat ineffective.

From the game tree in Figure 5, we can solve for the upper bound on q as a function of p. If the user makes the threat, there is a probability of p that the provider is hard and will defy the threat and the user gets a payoff of $3-2q$. With probability of $1-p$, the user meets a soft provider, which is assumed to comply to the threat giving a payoff of 4. Therefore, the expected payoff to the user from deploying the probabilistic threat is $p(3-2q)+4(1-p)=-2pq-p+4$.

If, on the other hand, the user refrains from making the threat, it gets a payoff of 3. Therefore, for the threat to work, $-2pq-p+4>3$, or $q<\frac{1-p}{2p}$. This upper bound on q is called the *acceptability condition*. It is called so, because if the q is greater than this expression, the user is better off not making any threats.

It is now clear that if the threat is to work, it must satisfy both the *effectiveness* and the *acceptability* conditions. Figure 6, which shows the equilibrium solution set, can be used by a user to design an effective and acceptable threat. For a threat to be credible to the provider, the associated (p,q) should be above the $q=0.5$ line. Similarly, for the risk of threat to be acceptable to the user, the (p,q) must lie below the curve $q=\frac{1-p}{2p}$.

Figure 6 shows two important limits for p, P_L and P_U. P_L (=0.33) is the intersection of $q=1$ and $q=\frac{1-p}{2p}$, whereas P_U (=0.5) is the intersection of $q=0.5$ and $q=\frac{1-p}{2p}$. For $p=P_L$, we observe q assumes its maximum value of 1. Therefore, for $p<P_L$, the pure threat would work. However, for $P_L<p<P_U$, the pure threat would not work, but a probabilistic threat would. If p exceeds P_U, no values of q satisfies both conditions. Therefore, the user would not gain by threatening to quit when $p>P_U$; the user must adopt other strategies to secure a better quality communication.

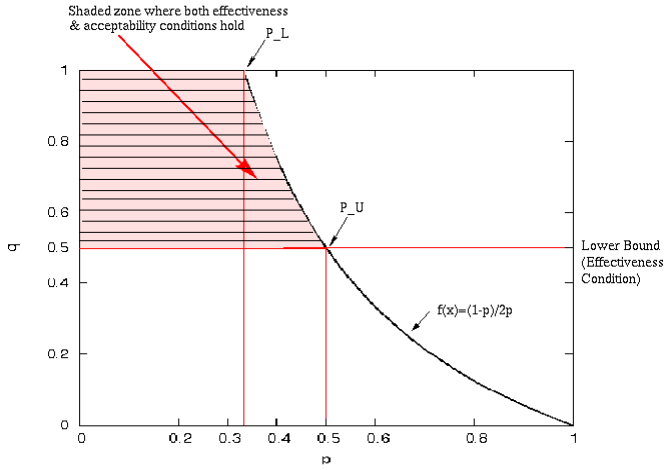


Fig. 6. Conditions of Successful Brinkmanship

IV. Generalization of Brinkmanship Model

In the previous section, we used a set of specific payoff cardinal values to construct an example game of brinkmanship. Using that specific example, we were able to explain four key conditions of brinkmanship, the effectiveness condition, the acceptability condition, condition under which a pure threat can be effective and acceptable, condition under which a pure threat could be too risky but a probabilistic threat can be both acceptable and effective, and finally the condition under which it is not possible for the user to issue a threat that is both acceptable and effective. In this section, we first generalize the brinkmanship model by using variables, instead of specific cardinal values, for the payoffs, and later prove a set of theorems which generalizes these conditions.

The payoff variables are defined in Table I along with their ordinal rankings. For the purposes of minimizing the total number of variables, we use the same set of variables, m and s, for both hard and soft providers to denote compliance and defiance payoffs. With the ordinal ranking ($m < s$) preserved for these two variables, we can effectively model compliance and defiance payoffs for hard and soft providers by switching their use as shown in Table I. This is possible because we know that the payoff for a soft provider complying to a threat is higher than that when he denies, which is opposite to the payoffs for a hard provider.

TABLE I
Payoff Cardinals

Player	Payoff Variables	Ordinal Ranking
User	x: Provider defies threat y: User does not threaten z: Provider complies to threat	$x < y < z$
Provider	m: Hard provider complies or Soft provider defies s: Hard provider defies or Soft provider complies r: User does not threaten (Hard/Soft)	$m < s < r$

Theorem 1: If the provider payoff ordinal rankings are given by Table I, and if the user leaves the provider with probability q in the event the threat is not complied, the *effectiveness condition* is given by:

$$q > \frac{r-s}{r-m} \tag{1}$$

Proof 1: For a threat to be effective, the provider must find that his payoff for compliance is greater than defiance. This cannot happen with a hard provider, because his defiance payoff, $qs + r(1-q)$ is always greater than his compliance payoff of m for any values of $0 \leq q \leq 1$. Therefore, the hard provider will always defy the threat. The threat can be effective only if the soft provider complies, which happens when:

$$s > qm + r(1-q)$$
$$or, q > \frac{r-s}{r-m} \quad \blacksquare$$

Theorem 2: If the user payoff ordinal rankings are given by Table I, the probability that the provider is hard is given by p, and the probability of the user leaving the provider if the threat is not complied is given by q, then the *acceptability condition* is:

$$q < \frac{(1-p)(z-y)}{p(y-x)} \tag{2}$$

Proof 2: For the threat to be rewardable to the user, the expected payoff from threatening the provider should be larger than the payoff of not threatening (y). Therefore,

$$p\{qx + y(1-q)\} + z(1-p) > y$$
$$q < \frac{(1-p)(z-y)}{p(y-x)} \quad \blacksquare$$

Theorem 3: If the user payoff ordinal rankings are given by Table I, the probability that the provider is hard is given by p, and the probability of the user leaving the provider if the threat is not complied is given by q, then the *lower bound* of p (P_L) is given by:

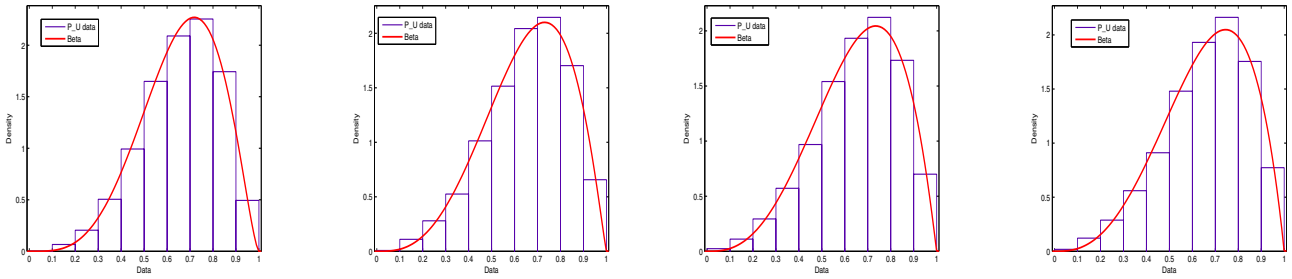
$$P_L = \frac{z-y}{z-x} \tag{3}$$

Proof 3: P_L can be found by equating the right hand side of Condition (2) to 1 (see Figure 6):

$$1 = \frac{(1-p)(z-y)}{p(y-x)}$$
$$or, p = \frac{z-y}{z-x} \quad \blacksquare$$

Theorem 4: If the user and provider payoff ordinal rankings are given by Table I, the probability that the provider is hard is given by p, and the probability of the user leaving the provider if the threat is not complied is given by q, then the *upper bound* of p (P_U)is given by:

$$P_U = \frac{(r-m)(z-y)}{(r-s)(y-x) + (r-m)(z-y)} \tag{4}$$



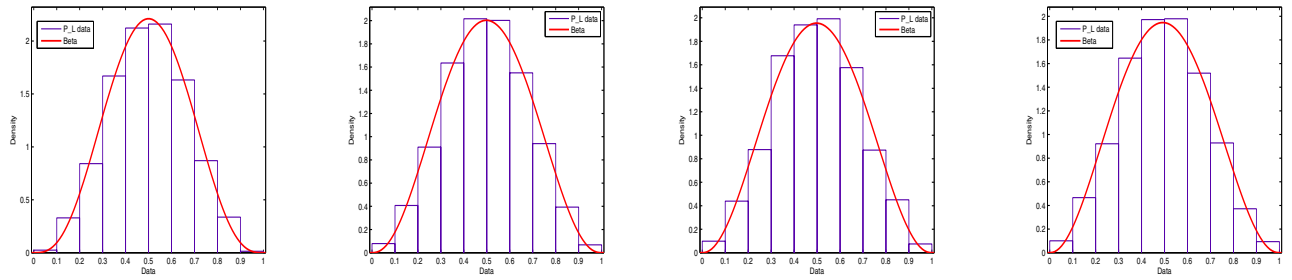
(a) P_U, Range of Payoff Cardinals=10, α=4.75386, β=2.46978, Skewness=-0.4145

(b) P_U, Range of Payoff Cardinals=20, α=4.04024, β=2.12003, Skewness=-0.4303

(c) P_U, Range of Payoff Cardinals=30, α=3.82103, β=2.01824, Skewness=-0.4331

(d) P_U, Range of Payoff Cardinals=40, α=3.70511, β= 1.99377, Skewness=-0.4234

Fig. 7. Upper Bounds of P (P_U), fitted with Beta Distribution



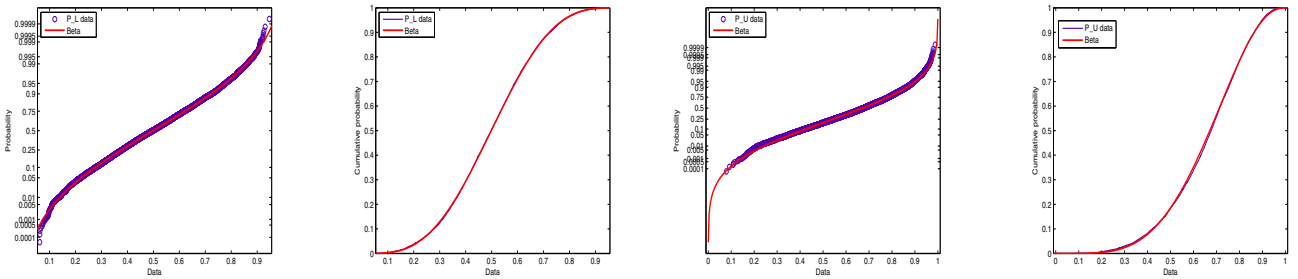
(a) P_L, Range of Payoff Cardinals=10, α=4.08112, β=4.08193, Skewness=0.0001

(b) P_L, Range of Payoff Cardinals=20, α=3.38291, β=3.40135, Skewness=0.0035

(c) P_L, Range of Payoff Cardinals=30, α=3.22998, β=3.25294, Skewness=0.0046

(d) P_L, Range of Payoff Cardinals=40, α=3.18179, β=3.25193, Skewness=0.0141

Fig. 8. Lower Bounds of P (P_L), fitted with Beta Distribution



(a) Probability Plot of P_L and fitted Beta Distribution

(b) Respective CDF of P_L and fitted Beta Distribution

(c) Probability Plot of P_U and fitted Beta Distribution

(d) Respective CDF of P_U and fitted Beta Distribution

Fig. 9. Demonstrative graphs showing the Goodness of the Distribution Fitting (Range of Payoff Cardinals=10)

Proof 4: P_U is found by equating the right hand sides of Conditions (1) and (2):

$$\frac{r-s}{r-m} = \frac{(1-p)(z-y)}{p(y-x)}$$
$$or, p = \frac{(r-m)(z-y)}{(r-s)(y-x)+(r-m)(z-y)} \quad \blacksquare$$

Theorems 3 specifies the condition under which a pure threat can be both acceptable and effective. Similarly, Theorem 4 stipulates the condition under which it is not possible for the user to issue a threat that is both acceptable and effective. However, we can see that these conditions are directly dependent on the payoff cardinals (P_L depends on user payoffs and P_U depends on both user and provider payoffs). In the following section, we investigate possible distributions of P_L and P_U for a large sample space where payoffs are generated randomly within their specified ranges.

V. Monte Carlo Simulation

In this section, we carry out Monte Carlo simulation [10] to gain a sense of the overall applicability of the brinkmanship

concept in wireless networking given that the user and provider payoff values are quite uncertain. Specifically, our goal is to study the behaviour of the two critical variables, P_U and P_L, over a large random sample space. We conducted a set of four Monte Carlo simulations each comprising of $10,000$ sampling instances. For a given sample, random values were drawn for each of the six payoff variables, x, y, z, m, s, r, from their respective ranges. We considered four different successively larger non-overlapping ranges, 10, 20, 30, and 40 (see Column 1 in Table II for the four sets of simulation experiments). The ranges were chosen to be non-overlapping to ensure that the ordinal rankings of the payoff values are not violated.

Each simulation yields a set of 10,000 values for both P_U and P_L. Since both of these parameters are probability values and restricted between 0 and 1, a natural choice was to consider fitting the Beta distribution [11]. Beta distribution is a family of continuous probability distributions defined on the interval of $0, 1$, and is parameterized by two positive *shape parameters*, typically denoted by α and β. The values of α and β dictates the four distinct shapes of the frequency curves: Single peak ($\alpha > 1$ and $\beta > 1$), J-Shape ($\alpha < 1$ and $\beta > 1$), Reverse J ($\alpha > 1$ and $\beta < 1$), and U-Shape ($\alpha < 1$ and $\beta < 1$).

TABLE II
PROBABILITY OF ACCEPTABLE AND EFFECTIVE BRINKMANSHIP

Range and Payoff Cardinals	α, β	Mean	$Pr(P_U \geq 0.1)$
Range = 10 x(min,max)=(-9,0) y(min,max)=(1,10) z(min,max)=(11,20) m(min,max)=(-9,0) s(min,max)=(1,10) r(min,max)=(11,20)	P_U: 4.75386, 2.46978 P_L: 4.08112, 4.08112	P_U : 0.658098 P_L: 0.49995	P_U : 0.99983 P_L: 0.99751
Range = 20 x(min,max)=(-9,10) y(min,max)=(11,30) z(min,max)=(31,50) m(min,max)=(-9,10) s(min,max)=(11,30) r(min,max)=(31,50)	P_U: 4.04024, 2.12003 P_L: 3.38291, 3.40135	P_U: 0.655854 P_L: 0.498641	P_U: 0.99951 P_L: 0.99442
Range = 30 x(min,max)=(-9,20) y(min,max)=(21,50) z(min,max)=(51,80) m(min,max)=(-9,20) s(min,max)=(21,50) r(min,max)=(51,80)	P_U: 3.82103, 2.01824 P_L: 3.22998, 3.25294	P_U: 0.654368 P_L: 0.498229	P_U: 0.99932 P_L: 0.99333
Range = 40 x(min,max)=(-9,30) y(min,max)=(31,70) z(min,max)=(71,110) m(min,max)=(-9,30) s(min,max)=(31,70) r(min,max)=(71,110)	P_U: 3.70511, 1.99377 P_L: 3.18179 , 3.25193	P_U: 0.650148 P_L: 0.494549	P_U: 0.99915 P_L: 0.99272

The distribution fitting was achieved in **Matlab** using the `dfittool()` function, which takes the 10,000 data values for either P_U or P_L as obtained from the Monte Carlo simulation, constructs the probability density of the actual data, and then fits the Beta distribution to it. The distribution fitting basically involves deriving the values of the shape parameters, α and β, which best fit the probability density of the 10,000 data. For the four payoff ranges, Figures 7 and 8 show the fitting for P_U and P_L, respectively. All our achieved fittings matched very well with the simulation data; for demonstration purpose, we show the probability plots and CDF plots of P_U and P_L along with their respective fitted Beta Distribution functions in Figure 9. We make the following observations:

- Irrespective of the ranges chosen for the payoff variables, both P_U and P_L are Beta distributed with the Single Peak shape ($\alpha > 1$, $\beta > 1$).
- The only effect of the payoff range is a slight decrease in the shape values α and β, but decrease is too small for the shape to be visually different.
- The shape of P_L distribution is symmetric (mean = 0.5), whereas the P_U distribution is left-skewed (i.e., it has a negative skew, The left tail is longer, meaning it has relatively few low values) with mean near 0.65.

Now let us discuss the implications of these observations. Most wireless network providers dimension their networks to keep the blocking probability below 10% to ensure an acceptable level of quality of service. This means that when a threat is received, the probability that the provider has no available resources is about 0.1, i.e., we have $p = 0.1$. Therefore, for $P_L > 0.1$, the pure threat would work. A probabilistic threat would work for $P_L < 0.1 < P_U$. For $P_U < 0.1$, the user will not find any value for q that will satisfy both effectiveness and acceptability conditions and hence the user will not be able to help herself with the brinkmanship strategy.

Using the CDF of the fitted Beta distributions, Table II shows the probability of $P_U \geq 0.1$ for four different payoff ranges. We can see that irrespective of the payoff range, the chance for P_U to be greater than 0.1 is about 99.9%. This means that there is a 99.9% chance that the user will be able to issue a threat, either pure or probabilistic, that is both effective and acceptable.

VI. ACHIEVING THREAT CREDIBILITY: A PRACTICAL PERSPECTIVE

Now that the theoretical underpinnings for applying brinkmanship in pursuit of securing better quality wireless services from the providers are established, we turn our focus to the engineering issues involved in accommodating brinkmanship in the existing mobile communication systems. Threat credibility is a particular issue that must be adequately addressed in any practical system. If the user remains in total control of terminating (or not terminating) the current session, a threat would not be credible to the provider, because the user could then always decide not to carry out a threat should the provider defies (the user could simply 'bluff' the provider). Any practical system therefore must have some mechanism that takes session termination control away from the user once the user issues a threat to the provider.

Today's mobile phones have the capability of running a wide range of advanced applications which were beyond our

imagination only a few years ago. We discuss a possible mobile phone application for brinkmanship. The functional architecture of this application is shown in Figure 10. It has the following components:

- **Threat transmitter:** This entity allows the user to communicate a threat to the provider. A threat button can be used by the user to manually issue a threat to the provider. Upon pressing this button, a *threat signal* will be transmitted to the provider's wireless bases station (BS) using one of the existing signalling channels. Upon receiving a threat signal, the BS immediately transmits an acknowledgement signal (ACK). The handset will confirm the successful communication of the threat, using a light, a beep, or other appropriate mechanisms, only after it receives the ACK. If it does not receive the ACK for a timeout period, it will retransmit the threat signal until it receives an ACK.
- **Threat executor:** After successful deployment of a threat, the control is delegated to this entity. Delegation of control helps establish the credibility of the deployed threat, without which the threat may not be effective. The main function of this entity is to carry out the threat in the event the provider defies the threat. It implements a mechanism that can establish whether the provider has complied or defied. For this purpose, it communicates with the *channel monitor*. If defiance is detected, the threat executor will automatically terminate the current session and communicate the execution of the threat to the user via appropriate auditory or visual channels. If compliance is detected, the session is not terminated and the compliance is communicated to the user. Note that the threat executor must be implemented using 'tamper proof' technology [12] to prevent a user from tampering with these functions and cheat.
- **Channel monitor:** It monitors the quality of the communication channel, e.g., received signal strength, packet loss rates, etc. These parameters give an indication of the quality of the channel.

The architecture we discussed serves as an example to demonstrate that we already have the technological advancement to accommodate brinkmanship in existing mobile communication systems. This is by no means the optimum implementation solution. For example, one improvement could be to investigate 'policy-based threats', which replaces the 'threat button'. Users can enter their threat policies once, and the system can automatically issue threats according to these policies, relieving the user from interacting with the threat button in the middle of a session.

VII. Conclusion and Future Work

We have considered a scenario where mobile users may use threat as a strategic tool to force service providers allocating more resource to fix occasional link quality problems during an active communication session. The effectiveness and feasibility of the proposed threat-based mobile communication scenario was analysed using Game Theory and Monte Carlo simulation. Our analysis showed that, at least from a conceptual point of view, users can benefit from the dynamics of such a system. Using an example architecture, we have explained how the idea of a 'threat model' can be realised in practical mobile communication systems. We acknowledge that the contributions are theoretical, but nevertheless motivational for the idea of using threats as a potential solution to quality problems in competitive wireless networks. To fully analyse the benefits of the proposed threat model, practical implementations and trials with real users will be needed, which would be an interesting future work.

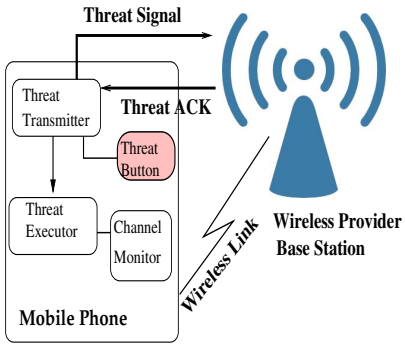


Fig. 10. A Mobile Phone Application for Brinkmanship

Acknowledgements

This research is funded by the Australian Research Council Discovery Project DP0881553.

References

[1] "Dual Sim Homepage. URL: http://www.dualsimmobilephones.com.au/, accessed on 3 December 2009."

[2] A. Nyandoro, L. Libman, and M. Hassan, "Service Differentiation Using the Capture Effect in 802.11 Wireless LANs," *IEEE Transactions on Wireless Communications*, vol. 6, no. 8, pp. 2961–2971, Aug. 2007.

[3] E. Altman, C. Barakat, and V. M. R. R., "Queueing analysis of simple FEC schemes for IP telephony," in *Proceedings of IEEE INFOCOM*, 2001, pp. 796–804.

[4] A. Dixit, D. Reiley, and S. Skeath, *Games of Strategy*, 3rd ed. W.W. Norton and Co., 2009.

[5] I. M. Suliman, C. Pomalaza-Ráez, I. Oppermann, and J. Lehtomäki, "Radio resource allocation in heterogeneous wireless networks using cooperative games," in *Proceedings Nordic Radio Symposium 2004 / Finnish Wireless Communications Workshop 2004*, 2004.

[6] M. Chatterjee, H. Lin, and S. K. Das, "Non-cooperative games for service differentiation in cdma systems," *Mob. Netw. Appl.*, vol. 10, no. 6, pp. 939–946, 2005.

[7] E. H. Watanabe, D. S. Menasche, E. de Souza e Silva, and R. M. M. Leao, "Modeling resource sharing dynamics of voip users over a wlan using a game-theoretic approach," in *Proceedings of IEEE INFOCOM*, 2008, pp. 915–923.

[8] K. S. Munasinghe, M. R. Kibria, and A. Jamalipour, "Designing voip session management over interworked wlan-3g cellular networks," *IEEE Wireless Communications*, vol. 15, no. 4, pp. 86–94, Aug. 2008.

[9] F. Melese and D. Angelis, "A brinkmanship game theory model of terrorism," in *Proceedings of the Third Conference on Mathematical Methods in Counterterrorism (CMMC)*, 2006.

[10] P. Robert and G. Xasella, *Monte Carlo Statistical Methods (Springer Texts in Statistics)*. Springer-Verlag New York, Inc., 2005.

[11] B. G. Barry and A. M. Carleton, *Synoptic and dynamic climatology*, 1st ed. Routledge, 2001.

[12] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: Design challenges," *ACM Transactions on Embedded Computing Systems*, vol. 3, no. 3, pp. 461–491, Aug. 2004.